

Claims

1. A method for tracing an instrumented program on a processor having an x86 architecture, comprising:
 - triggering a probe in the instrumented program;
 - obtaining an original instruction associated with the probe;
 - loading the original instruction into a scratch space;
 - loading a jump instruction for the x86 architecture into the scratch space wherein the jump instruction includes a next program counter value;
 - executing the original instruction in the scratch space using a thread; and
 - executing the jump instruction in the scratch space using the thread.
2. The method of claim 1, further comprising:
 - emulating the original instruction to determine a program counter value if the original instruction is a control-flow instruction; and
 - returning control to the thread at an address of the program counter value if the original instruction is a control-flow instruction.
3. The method of claim 1, further comprising:
 - determining the next program counter value by incrementing a value of a program counter using a size of the original instruction.
4. The method of claim 1, wherein the probe corresponds to a trap.
5. The method of claim 1, wherein obtaining the original instruction comprises:
 - searching a look-up table using a program counter value, wherein the look-up table comprises the original instruction associated with the probe and an address associated with the original instruction.
6. The method of claim 1, wherein the scratch space is allocated on a per-thread basis.

7. The method of claim 1, wherein the instrumented program is executed on a multi-thread architecture.
8. A system for tracing an instrumented program on a processor having an x86 architecture, comprising:
 - a thread configured to execute the instrumented program;
 - a look-up table arranged to store an address and a corresponding original instruction;
 - a trap handler configured to halt execution of the thread when a trap instruction is encountered, use an address of the trap instruction to obtain the corresponding original instruction from the look-up table, and generate a jump instruction to an address in the instrumented program;
 - a scratch space arranged to store the original instruction and the jump instruction; and
 - an execution facility for executing the original instruction to collect data and executing the jump instruction, wherein the execution facility is a processor based on the x86 architecture.
9. The system of claim 8, further comprising:
 - a buffer for storing the data.
10. The system of claim 8, further comprising:
 - a tracing framework configured to emulate the original instruction to determine a value of a program counter if the original instruction is a control-flow instruction and to return control to a thread at an address of the program counter value if the original instruction is a control-flow instruction.
11. The system to claim 8, wherein the trap handler sets a destination of the jump instruction to a next address immediately following an address of the trap instruction.
12. The system of claim 8, wherein the scratch space is allocated on a per-thread basis.
13. The system of claim 8, wherein the instrumented program is executed on multi-thread architecture.